

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA,	:	CRIMINAL NO.
	:	
v.	:	
	:	
MICHAEL EZEAGBOR,	:	
Defendant.	:	

STATEMENT OF OFFENSE

The parties in this case, the United States of America and the defendant, Michael Ezeagbor, stipulate and agree that the following facts are true and accurate. These facts do not constitute all of the facts known to the parties concerning the charged offense; they are being submitted to demonstrate that sufficient facts exist that the defendant committed the offense to which he is pleading guilty: Possession of Child Pornography, in violation of 18 U.S.C. Section 2252(a)(4).

STATEMENT OF FACTS

The Tor Network

Tor is a computer network which anonymizes Internet activity by routing a user's communications through a global network of relay computers (or proxies), thus effectively masking the internet-protocol ("IP") address of the user. An "IP address" is a unique numeric address (used by computers on the internet) that is assigned to properly direct internet traffic. A publically visible IP address can allow for the identification of the user and his/her location. To access the Tor network, a user has to install freely available Tor software, which relays only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address. There is no practical method to trace a user's actual IP address back through those Tor relay computers.

The Tor network makes it possible for a user to operate a special type of website, called “hidden services,” which uses a web address that is comprised of a series of 16 algorithm-generated characters (such as “asdlk8fs9dfiku7f”) followed by the suffix “.onion.” Websites, including hidden services, have system administrator(s) (also called the “admin(s)”) who are responsible for overseeing and operating these websites.

Bitcoin

Bitcoin (“BTC”) is one type of virtual currency that is circulated over the Internet. BTC is not issued by any government, bank, or company but rather is controlled through computer software. Generally, BTC is sent and received using a BTC “address,” which is like a bank account number and is represented by a case-sensitive string of numbers and letters. Each BTC address is controlled through the use of a unique private key, a cryptographic equivalent of a password. Users can operate multiple BTC addresses at any given time, with the possibility of using a unique BTC address for every transaction.

BTC fluctuates in value. Around March 5, 2018, one BTC was worth approximately \$11,573.00. A typical user purchases BTC from a BTC virtual-currency exchange, which is a business that allows customers to trade virtual currencies for conventional money (*e.g.*, U.S. dollars, euros, etc.). Little to no personally identifiable information about the sender or recipient is transmitted in a BTC transaction itself. However, virtual currency exchanges are required by U.S. law to collect identifying information of their customers and verify their clients’ identities.

To send BTC to another address, the sender transmits a transaction announcement, cryptographically signed with the sender’s private key, across the BTC network. Once the sender’s transaction announcement is verified, the transaction is added to the blockchain. The blockchain is a decentralized, public ledger that logs every BTC transaction. In some instances, blockchain

analysis can reveal whether multiple BTC addresses are controlled by the same individual or entity. For example, analyzing the data underlying BTC transactions allowed for the creation of large databases that grouped BTC transactions into “clusters.” This analysis allowed for the identification of BTC addresses that were involved in transacting with the same addresses.

THE WEBSITE

“The Website” was a website dedicated to the advertisement and distribution of child pornography that operated as a hidden service on the Tor network until March of 2018 when it was seized by law enforcement. The Website was used to host and distribute video files depicting child pornography that could be downloaded by site users. The Website was not intended to be used to upload pornography of adults, as evidenced on the upload page on The Website which clearly stated: “Do not upload adult porn.” The Website server had over 250,000 unique video files, which totaled approximately eight terabytes of data.

Any user could create a free account on The Website by creating a username and password. Only after the user registered an account could the user browse previews of videos available for download and post text to The Website. To download videos from the site, users used “points,” which were allocated to users by The Website. A registered user could earn points from The Website in several ways: (1) uploading videos depicting child pornography; (2) referring new users to The Website; (3) paying for a “VIP” account, which lasted for six months, entitled a user to unlimited downloads, and was priced at 0.03 BTC (approximately \$327.60 as of March 1, 2018); or (4) paying for points incrementally (*i.e.*, .02 BTC for 230 points). Points were not transferable to any other website or application. Once a customer sent BTC to The Website, the BTC could not be refunded or redirected. The points obtained by the payment of BTC could only be used for downloading videos.

Certain persons joined the conspiracy to distribute child pornography by uploading videos to The Website. Those co-conspirators who uploaded videos of child pornography to The Website for “points” also earned additional “points” each time a customer of the site downloaded that particular video from The Website. Thus, the co-conspirators had a shared goal as part of the conspiracy – increasing the number of unique videos on The Website to drive additional traffic to it, which in turn led to greater downloads and more points for the co-conspirators. When uploading videos, the co-conspirators would use explicit file names highlighting the content as showing the sexual exploitation of minors and would add tags that customers could search for, such as PTHC, 2yo, etc. In order to prevent duplicate videos from being uploaded, The Website operated a digital hash-value check of videos the co-conspirators uploaded in order to compare the video to other videos previously uploaded to the site. The Website did not allow a co-conspirator to upload a video whose hash value matched something previously uploaded to the site.

During the course of the investigation, law enforcement agents in Washington, D.C. accessed The Website on multiple occasions, including on or about September 28, 2017, February 8, 2018, and February 22, 2018, observed its functionality by browsing the listings on The Website, and conducted undercover purchases by downloading child pornography video files from The Website. These downloaded child pornography video files included pre-pubescent children, infants, and toddlers engaged in sexually explicit conduct. Each video available for download from The Website had a title, a description (if added by the co-conspirator), “tags” with further descriptions of the video enabling a user to more easily locate a particular category of video using The Website’s search function, and a preview thumbnail image that contained approximately sixteen unique still images from the video.

On or about March 5, 2018, South Korean law enforcement executed a search warrant at the residence of the administrator of The Website in South Korea. Pursuant to the search, South Korean law enforcement seized The Website's server and associated electronic storage media. South Korean law enforcement then provided to U.S. law enforcement a forensic image of the server. U.S. law enforcement subsequently obtained a federal search warrant to review this forensic image.

IDENTIFICATION OF THE DEFENDANT (a/k/a MIKEXP1)

A review of the forensic image of the server revealed a transfer of approximately 0.1 BTC (worth about \$38.00) on January 29, 2016 from a BTC address to The Website's BTC address starting with 1BwB. Subpoena returns from a virtual-currency exchange in the United States ("BTC Exchange") revealed that the source of this BTC transfer was from BTC Exchange Account number starting with 528a ("Subject BTC Exchange Account"). The defendant, EZEAGBOR, made that payment to The Website.

Law enforcement's review of the forensic image of the server revealed that The Website created the BTC address starting with 1BwB for a user account in the name of mikexp1. A review of mikexp1's account revealed that between approximately January 28, 2016 and February 19, 2016, mikexp1 downloaded approximately 42 videos from The Website with video file names and descriptions indicative of child pornography. Additionally, from approximately November 25, 2015 to January 25, 2016, mikexp1 uploaded approximately 10 videos of child pornography to The Website. The defendant, EZEAGBOR, downloaded those approximately 42 videos and uploaded those approximately 10 videos, all of child pornography, to The Website.

The videos possessed and uploaded to The Website by the defendant under the moniker mikeexp1 includes video file scara2_00172.avi with file description "Girl." The video is almost

fourteen minutes long. The video starts with a message which reads, “13 red my cap so hot” and contains a collage of photographs depicting a clothed female child, approximately ten to thirteen years old, sitting in front of a web camera. The child initially exposes her right breast to the camera and then removes her pants. The child appears to move the camera to face her pubic area and uses her fingers to masturbate her genitalia. Towards the end of the video, the child continues to masturbate herself by using her fingers and also inserts a crayon into her vagina.

Another video possessed and uploaded to The Website by the defendant under the moniker mikeexp1 includes video file scara2_00151.avi with file description “Girl.” The video is five minutes and thirty seconds and depicts a nude female child, approximately seven to ten years old. The child is posing in front of a web camera and switches between several sexually suggestive poses, including posing on her hands and knees while she positions her buttocks towards the camera and uses her hands to spread apart her buttocks to expose her genitalia. During the video, the child also sits in a chair facing the camera and spreads her legs to provide a close up view of her pubic area as she uses her fingers to expose her genitalia

Subpoena returns from the BTC Exchange revealed that the Subject BTC Exchange Account (which sent BTC to The Website) was created on or about November 18, 2013 with the following know-your-customer data:

- registered in the name of MICHAEL EZEAGBOR;
- with EZEAGBOR’s true date of birth in 1996;
- with EZEAGBOR’s true address in Texas;
- using EZEAGBOR’s true Social Security number;
- EZEAGBOR’s true phone number; and
- an email address of michaelenzeagbor@[X].com.

The defendant, EZEAGBOR, created that Subject BTC Exchange Account and funded it from his bank account as described below.

Subpoena returns from Yahoo revealed that the email address of michaelenzeagbor@[X].com was created on February 3, 2008 and also is registered to “Mr. Michael Ezeagbor” with the same telephone number that the defendant provided when he created the Subject BTC Exchange Account. The Yahoo account also provided a postal code of 78660, which is the same postal code provided by the defendant when he created the Subject BTC Exchange Account on January 29, 2016.

The Subject BTC Exchange Account was funded by an A+ Federal Credit Union (“A+FCU”) checking account ending in 7569 and a A+FCU debit card ending in 2098. Subpoena returns revealed that both of these payment methods were listed in the defendant’s name. The subpoena returns further revealed that the defendant opened the account ending in 7569 in 2012. The defendant provided the same date of birth, social security number, home address, and email address when he opened this A+FCU bank account that he had provided to the BTC Exchange when he opened the Subject BTC Exchange Account. Additionally, subsequent law enforcement investigation identified counter security footage from A+FCU on December 4, 2017, which shows an individual resembling the defendant’s driver’s license photograph accessing his account.

ARREST OF THE DEFENDANT

On January 9, 2019, the defendant was arrested by law enforcement at his residence in the Western District of Texas. At the time of his arrest, the defendant waived his rights and admitted to accessing The Website and downloading child pornography using the name “mikexpl.” Law enforcement also executed a search warrant at the defendant’s residence and seized several electronic devices, including computers, data storage devices, and a mobile phone.

A subsequent forensic analysis on the devices seized from the defendant’s residence identified approximately 190 images and approximately 14 videos depicting child pornography.

The National Center for Missing and Exploited Children (NCMEC) determined that at least 56 images and 2 videos of child pornography depicted at least 8 known child victims.

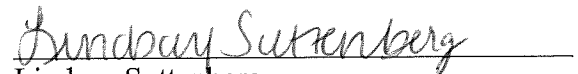
CONCLUSION

The defendant knowingly possessed one or more computers and electronic devices that contained one or more images and videos of child pornography in digital format, and knowingly possessed said child pornography. These visual depictions of child pornography had been shipped and transported in interstate and foreign commerce and using a means and facility of interstate and foreign commerce, including by computer, and/or were produced using materials that had been shipped and transported in and affecting interstate and foreign commerce, including by computer. The production of these visual depictions involved the use of one or more minors engaging in sexually explicit conduct. The visual depictions of child pornography were of one or more children under the age of eighteen (18) years engaging in such sexually explicit conduct. Specifically:

- One or more images and videos of child pornography possessed by the defendant involved a “prepubescent minor...who had not attained 12 years of age.” See U.S.S.G. 2G2.2(b)(2).
- The 10 videos the defendant uploaded to The Website were distributed for the “receipt of a thing of value, but not for pecuniary gain,” see U.S.S.G. 2G2.2(b)(3)(B), to wit: the defendant received points that he could only redeem on The Website for downloading additional videos depicting child pornography;
- In total the defendant possessed approximately 190 images and approximately 65 videos depicting child pornography. Accordingly, the offense involved “600 or more images.” See U.S.S.G. 2G2.2(b)(7)(D); see also Application Note 4(B)(ii) (“each video...shall be considered to have 75 images.”)

Respectfully submitted,

JESSIE K. LIU
UNITED STATES ATTORNEY


Lindsay Suttenger
Assistant United States Attorneys

DEFENDANT'S ACKNOWLEDGMENT

I have read every page of this Statement of the Offense and have discussed it with my attorney. I fully understand this Statement of the Offense. I agree and acknowledge by my signature that this Statement of the Offense is true and accurate. I do this voluntarily and of my own free will. No threats have been made to me nor am I under the influence of anything that could impede my ability to understand this Statement of the Offense fully.

Date: 5/15/2019

me
Michael Ezeagbor
Defendant

ATTORNEY'S ACKNOWLEDGMENT

I have read every page of this Statement of the Offense, and have reviewed it with my client fully. I concur in my client's desire to adopt this Statement of the Offense as true and accurate.

Date: _____

Joanne Slaight
Defense Counsel

Date: 5.15.2019

[Signature]
David Peterson
Defense Counsel